Docket No.: 62807-159 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Katsuyuki UMEZAWA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: January 30, 2004	:	Examiner:

For: CERTIFICATE MANAGEMENT SYSTEM AND METHOD

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. JP 2003-402401, filed on December 2, 2003.

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Reg No. 36,139

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:gav
Facsimile: (202) 756-8087
Date: January 30, 2004

62807-159

[redacted]

January 30, 2004
Katsuyuki UMEZAWA, etc.

McDermott, Will & Emery

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１２月　２日

出願番号
Application Number: 特願２００３－４０２４０１

[ST. 10/C]: [ＪＰ２００３－４０２４０１]

出願人
Applicant(s): 株式会社日立製作所

２００４年　１月１９日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０００６９４

【書類名】　特許願
【整理番号】　K03010081A
【あて先】　特許庁長官殿
【国際特許分類】　G06K 17/00
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　梅澤　克之
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　内山　宏樹
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内
　【氏名】　洲崎　誠一
【発明者】
　【住所又は居所】　神奈川県川崎市幸区鹿島田８９０番地　株式会社日立製作所情報・通信グループ内
　【氏名】　児玉　俊臣
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100075096
　【弁理士】
　【氏名又は名称】　作田　康夫
【選任した代理人】
　【識別番号】　100100310
　【弁理士】
　【氏名又は名称】　井上　学
【手数料の表示】
　【予納台帳番号】　013088
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1

【書類名】特許請求の範囲
【請求項１】
公開鍵証明書の管理システムであって，
提示された公開鍵証明書の有効性を検証し，検証が正しく行えた場合にサービスを提供する，サービス提供者装置と，前記サービス提供者装置が信頼する認証局装置と，ＩＣカードと，からなり，
前記ＩＣカードは，
前記認証局装置に対する証明書を発行するために必要な，第１の秘密鍵とその対となる第１の公開鍵と，前記第１の公開鍵に対して発行された第１の証明書と，
前記サービス提供者装置からサービスを受けるために生成する，第２の秘密鍵とその対となる第２の公開鍵と，
前記第２の公開鍵に対して，前記サービス提供者装置が信頼する前記認証局装置により発行される第２の証明書と，を記憶する記憶部と，
前記第１，第２の公開鍵と第１，第２の秘密鍵とを生成する鍵生成部と，
を備え，
前記認証局装置は，
前記ＩＣカードに対して前記第２の公開鍵の証明書を生成するための，第３の秘密鍵とその対となる第３の公開鍵に対して発行される前記証明書と，を記憶する記憶部と，
発行申請に基づき，第２の公開鍵に対する第２の証明書を生成する証明書生成部と，
を備え，
前記ＩＣカードは，
前記認証局装置による証明書の発行要求に基づき，記憶している前記第１の秘密鍵を用いて，前記認証局装置の証明書を発行する証明書生成部と，
を備える
ことを，特徴とする証明書管理システム。
【請求項２】
請求項１記載の証明書管理システムであって，
前記認証局装置は，
証明書の失効申請に基づき，証明書の失効情報を生成する失効情報生成部と，
該失効情報生成部で生成した失効情報を保管する失効情報ＤＢと，を備えており，
前記ＩＣカードは，前記サービス提供者装置からサービスを受けるために，
前記第１の証明書と第２の証明書を前記サービス提供者装置に提示し，
前記サービス提供者装置は，
提示された前記第１，第２の証明書の有効性を検証する際に，前記第１の証明書と前記当該第２の証明書の失効情報を，前記認証局装置に問い合わせる証明書検証部，を備える。
【請求項３】
請求項１記載の証明書管理システムであって，
前記ＩＣカードは，
前記記憶部を，前記サービス提供者固有領域として構成し，
当該固有領域へのアクセスを，前記固有領域に対応する前記サービス提供者装置のみに許可するサービス提供者認証部を備える
ことを特徴とする証明書管理システム。
【請求項４】
請求項１記載の証明書管理システムであって，
前記ＩＣカードの，前記サービス提供者固有領域，および，証明書生成部に記憶されているデータは暗号化されている
ことを特徴とする証明書管理システム。
【請求項５】
請求項１記載の証明書管理システムであって，

証明書検証機関装置を備え，
前記証明書検証機関装置は，前記サービス提供者装置の，前記証明書検証部による証明書の有効性検証を，前記サービス提供者装置に代わって行う
ことを，特徴とする証明書管理システム。
【請求項６】
請求項１記載の証明書管理システムであって，
証明書保管機関装置を備え，
前記証明書保管機関装置は，前記ＩＣカード内に保存される複数の証明書を前記ＩＣカードに代わって保管し，要求に従い前記証明書を提供する
ことを，特徴とする証明書管理システム。
【請求項７】
請求項２記載の証明書管理システムであって，
証明書検証時に，
前記認証局装置が前記第２の証明書を検証する時に，
前記サービス提供者装置は，チャレンジを送信し，
前記ＩＣカードは，
前記第２の秘密鍵で，前記チャレンジを暗号化し，
該暗号化されたチャレンジと，前記第２の秘密鍵に対応した第２の証明書と，前記第１の秘密鍵に対応した第１の証明書と，を前記サービス提供者装置に送信し，
前記サービス提供者装置は，
前記暗号化されたチャレンジを復号化して前記ＩＣカードに送信した前記チャレンジと一致するかどうかを確認し，
受け取った前記第１の証明書と第２の証明書との失効情報を取得し，
取得した前記失効情報を用いて，前記第１，第２の証明書の検証処理を行う証明書検証部と，
検証処理において，前記第１，第２の証明書は有効である，と判断した場合に，サービスの提供を行うサービス提供部を備える
ことを特徴とする証明書管理システム。
【請求項８】
請求項７記載の証明書管理システムであって，
前記ＩＣカードは，
前記記憶部を，前記サービス提供者固有領域として構成し，
前記サービス提供者装置は，前記サービス提供者固有領域へのデータの送受信を行うときに，
前記サービス提供者固有領域との間で，相互認証処理を行う
ことを特徴とする証明書管理システム。
【請求項９】
請求項７記載の証明書管理システムであって，
前記ＩＣカードの，前記サービス提供者固有領域，および，証明書生成部へ，データを保存するときに，該データを暗号化した後で，保存することを特徴とする証明書管理システム。

【書類名】明細書
【発明の名称】証明書管理システムおよびその方法
【技術分野】
【０００１】
本発明は，ＩＣカード等の記憶媒体を用いた証明書管理方法に関し，さらに詳しくは，複数の証明書がＩＣカード等の記憶媒体に搭載される場合の，証明書失効を効率化するための証明書発行方法に関する。
【背景技術】
【０００２】
ＩＣカードに，サービス提供者装置ごとに領域を分けて，アプリケーションおよびデータを搭載する技術が知られている（例えば，非特許文献１参照。）。
【０００３】
また，ＩＣカードの利用者が公開鍵証明書を申請して取得し，取得した公開鍵証明書がＩＣカードに搭載され，実際に発行されるまでの仕組みを提供している技術もある（例えば，特許文献１参照）。
【０００４】
また，ＩＣカードに搭載された公開鍵や公開鍵証明書を安全に遠隔より書き換えるため仕組みを提供している技術もある（例えば，特許文献２参照）。
【０００５】
【特許文献１】特開２００２－２９８０８８号公報
【０００６】
【非特許文献１】「グローバルプラットフォームカードスペシフィケーションバージョン２．１（GlobalPlatform Card Specification Version2.1）」，（米国），グローバルプラットフォーム社（GlobalPlatform Inc.），２００１年６月，ｐ．２７
【特許文献２】米国特許出願公開第２００３／００５６０９９Ａ１号明細書
【発明の開示】
【発明が解決しようとする課題】
【０００７】
サービス提供者装置は，サービス提供時に，サービス利用者に，該サービス提供者装置が信頼する認証局装置から発行された証明書の提示を求め，該証明書が確かに，信頼する認証局装置から発行されたものかどうか，有効期限が切れていないかどうか，等の検証を行うことで，サービス利用者を認証することができる。
【０００８】
昨今普及しつつあるマルチアプリケーション搭載可能なＩＣカードに，複数のサービス提供者装置が，個別に，証明書および該証明書に対応する秘密鍵を搭載し，認証処理を行う場合を考える。
【０００９】
個々のサービス提供者装置は，１つの共通の認証局装置だけを信頼するのではなく，個別に認証局装置を信頼したい場合も考えられる。このような場合に，たとえば，ＩＣカードを無くしてしまったため，ＩＣカードの所有者が，ＩＣカードに搭載されているすべての証明書を失効させたい場合，すべてのサービス提供者に，あるいは，認証局に連絡しなければならず，効率が悪い。また，個々のサービス提供者装置が，自らが信頼する認証局装置から発行された証明書を，自らの権限で失効させたい場合もある。
【００１０】
従って，簡単でかつ柔軟な失効方法が求められている。
【課題を解決するための手段】
【００１１】
本発明は，上記事情に鑑みてなされたものであり，一つのサービス提供者装置（たとえばカード発行者等の第１のサービス提供者装置）に連絡し，該サービス提供者装置１が信頼する認証局装置から発行された証明書を失効するだけで，他のサービス提供者装置が信

頼する認証局装置から発行された証明書も同時に失効させることができる，証明書管理方法およびその方法が適用されるシステムを提供する。

【００１２】

また，複数のサービス提供者装置が，それぞれ異なる信頼する認証局装置から発行される証明書をＩＣカードに搭載しており，何らかの理由で，ある特定の証明書を失効させたい場合に，他の証明書は失効させずに，上記特定の証明書を個別に失効させることもできる，証明書管理方法およびその方法が適用されるシステムを提供する。

【００１３】

具体的には，上位の第１のサービス提供者装置が信頼する第１の認証局装置により発行されたＩＣカード内の第１の証明書を用いて，ＩＣカード内で，下位の第２のサービス提供者装置が信頼する，第２の認証局装置の証明書２’を生成し，さらに該証明書２’を用いて第２の認証局装置が第２の証明書を生成する，という階層的な証明書の連鎖を構成する。

【００１４】

このとき，第２のサービス提供者装置が複数で，それぞれ異なる第２の認証局装置を信頼し，複数の第２の認証局装置が，それぞれ第２の証明書を生成してもよい。

【００１５】

上記連鎖構成により，該下位の証明書２の有効性を検証するためには，上記証明書２’および上記証明書１の有効性の検証が必要となる。つまり，ＩＣカードを無くした等の理由により，証明書１および証明書２を失効させたい場合，サービス提供者装置１が信頼する認証局装置により発行された上位の証明書１を，失効させるだけで，一つ以上のサービス提供者装置２が信頼する一つ以上の認証局装置２が発行した一つ以上の下位の証明書２も失効させることができる。

【００１６】

一方，上記連鎖構成において，各証明書の検証時には，その発行元認証局が発行した失効情報を参照する構成とすることにより，個々の証明書を失効させることも可能である。例えば，サービス提供者装置２がサービスの提供を停止する場合などには，サービス提供者装置２が信頼する認証局装置による失効情報を発行させる。これにより，サービス提供者装置１が信頼する認証局装置１が発行した証明書１は有効のまま，サービス提供者装置２が信頼する認証局から発行された証明書２を，失効させることが可能となる。

【００１７】

本発明による証明書管理システムは，より具体的には，　提示された公開鍵証明書の有効性を検証し，検証が正しく行えた場合にサービスを提供する，サービス提供者装置と，上記サービス提供者装置が信頼する認証局装置と，ＩＣカードと，からなる。

【００１８】

そして，上記ＩＣカードは，上記認証局装置に対する証明書を発行するために必要な，第１の秘密鍵とその対となる第１の公開鍵と，上記第１の公開鍵に対して発行された第１の証明書と，上記サービス提供者装置からサービスを受けるために生成する，第２の秘密鍵とその対となる第２の公開鍵と，上記第２の公開鍵に対して，上記サービス提供者装置が信頼する上記認証局装置により発行される第２の証明書と，を記憶する記憶部と，上記第１，第２の公開鍵と第１，第２の秘密鍵とを生成する鍵生成部と，を備えることを特徴とする。

【００１９】

さらに，上記認証局装置は，上記ＩＣカードに対して上記第２の公開鍵の証明書を生成するための，第３の秘密鍵とその対となる第３の公開鍵に対して発行される上記証明書と，を記憶する記憶部と，発行申請に基づき，第２の公開鍵に対する第２の証明書を生成する証明書生成部と，を備えることを特徴とする。

【００２０】

さらに，上記ＩＣカードは，上記認証局装置による証明書の発行要求に基づき，記憶している上記第１の秘密鍵を用いて，上記認証局装置の証明書を発行する証明書生成部と，

を備えることを特徴とする。

【００２１】

また，上記証明書管理システムにおいて，上記認証局装置は，証明書の失効申請に基づき，証明書の失効情報を生成する失効情報生成部と，該失効情報生成部で生成した失効情報を保管する失効情報ＤＢと，を備え，上記ＩＣカードは，上記サービス提供者装置からサービスを受けるために，上記第１の証明書と第２の証明書を上記サービス提供者装置に提示し，上記サービス提供者装置は，提示された上記第１，第２の証明書の有効性を検証する際に，上記第１の証明書と上記当該第２の証明書の失効情報を，上記認証局装置に問い合わせる証明書検証部，を備えることを特徴とする。

【００２２】

また，上記証明書管理システムにおいて，証明書検証時に，上記認証局装置が上記第２の証明書を検証する時に，上記サービス提供者装置は，チャレンジを送信し，上記ＩＣカードは，上記第２の秘密鍵で，上記チャレンジを暗号化し，該暗号化されたチャレンジと，上記第２の秘密鍵に対応した第２の証明書と，上記第１の秘密鍵に対応した第１の証明書と，を上記サービス提供者装置に送信し，上記サービス提供者装置は，上記暗号化されたチャレンジを復号化して上記ＩＣカードに送信した上記チャレンジと一致するかどうかを確認し，受け取った上記第１の証明書と第２の証明書との失効情報を取得し，取得した上記失効情報を用いて，上記第１，第２の証明書の検証処理を行う証明書検証部と，検証処理において，上記第１，第２の証明書は有効である，と判断した場合に，サービスの提供を行うサービス提供部を備えることを特徴とする。

【発明の効果】

【００２３】

本発明によれば，複数のサービス提供者装置が，それぞれ異なる信頼する認証局装置から発行される証明書をシステムに搭載する場合に，簡単で，かつ柔軟な失効方法を備えた，証明書管理方法を提供することができる。

【発明を実施するための最良の形態】

【００２４】

本発明の一実施形態について説明する。なお，これにより本発明が限定されるものではない。

【００２５】

図１は，本発明の一実施形態が適用された証明書管理システムのネットワーク構成図である。

【００２６】

本実施形態の証明書管理システムは，図１に示すように，複数のサービス提供者装置４０$_1$～４０$_n$（以下，単にサービス提供者装置４０とも称する）と，クライアント端末２０（以下，単に端末２０とも称する）とがインターネットなどの通信網３０を介して，互いに接続されて構成されている。また端末２０は，ＩＣカード１０と接続される。またサービス提供者装置４０$_1$～４０$_n$は，それぞれ認証局装置５０$_1$～５０$_n$（以下，単に認証局装置５０とも称する）と接続されている。

【００２７】

認証局装置５０は，証明書の発行申請に基づき，証明書を発行し，また，証明書の失効申請に基づき，証明書失効情報を配布する。図２に示すように，認証局装置５０は，証明書を生成するための秘密鍵Ａ５０１と，該秘密鍵に対応した公開鍵証明書Ａ５０２と，証明書の発行申請に基づき，証明書を生成する証明書生成部５０２と，証明書の失効申請に基づき，証明書の失効情報を生成する失効情報生成部５０３と，該失効情報生成部で生成した失効情報を保管する失効情報ＤＢ５０４と，データの送受信を行う通信部５０１と，秘密鍵と該秘密鍵に対応する公開鍵を生成する鍵生成部５０５と，他の装置に対して証明書発行を依頼するための証明書発行申請を生成する証明書発行申請生成部５０６と，を含む。

【００２８】

サービス提供者装置４０は，提示された証明書の有効性を検証し，有効性検証が正しく行えた場合に，サービスを提供する。図３に示すように，サービス提供者装置４０は，提示された証明書の有効性を検証する証明書検証部４０２と，該証明書検証部により，有効性検証が正しく行えた場合に，サービスを提供するサービス提供部４０３と，データの送受信を行う通信部４０１と，を含む。

【００２９】

ＩＣカード１０は，上記サービス提供者４０毎の固有の領域を持ち，該領域に，上記サービス提供者４０の情報を保持し，また，証明書の発行要求に基づき，証明書を発行する。図４に示すように，ＩＣカード１０は，上記サービス提供者40_1～40_nの情報を保持するサービス提供者固有領域103_1～103_n（以下，サービス提供者固有領域１０３とも称する）と，証明書の発行要求に基づき，上記サービス提供者固有領域１０３に保持されている秘密鍵を用いて，証明書を発行する証明書生成部１０２と，外部とデータを送受信するデータ送受信部１０１と，秘密鍵と公開鍵のペアを生成する鍵生成部１０４と，秘密鍵を用いて暗号化を行う暗号化部１０５と，上記サービス提供者固有領域１０３に対応する上記サービス提供者装置４０を認証し，該サービス提供者装置４０のみにアクセスを許可するサービス提供者認証部１０６と，を含む。

【００３０】

端末２０は，上記サービス提供者装置４０からの要求を上記ＩＣカード１０に伝送し，また，上記ＩＣカード１０から情報を引き出し，上記サービス提供者装置４０に，該情報を伝送する。なお，サービス提供者固有領域103_1～103_nとの情報伝達は，上記サービス提供者認証部１０６のアクセス制御機能により，それぞれ対応するサービス提供者装置40_1～40_nしか実行できない。

【００３１】

図５に示すように，端末２０は，上記ＩＣカード１０とデータを送受信するＩＣカードアクセス部２０１と，上記サービス提供者装置４０と，あるいは，上記認証局装置５０と，データを送受信するデータ送受信部２０２と，を含む。

【００３２】

図６は端末２０のハードウェア構成図である。端末２０は，通信装置２１と，入出力装置２２と，ＩＣカード入出力装置２３と，記憶装置２４と，ＣＰＵ２５とメモリ２６と，読取装置２７とがバスなどの内部通信線２９で連結され，記憶媒体２８を含めて構成されている。また，端末２０はＩＣカード入出力装置２３を経由して，ＩＣカード１０とつながる。

【００３３】

サービス提供者装置４０および認証局装置５０のハードウェア構成は端末２０のハードウェア構成と同様である。ただし，サービス提供者装置４０および認証局装置５０が，直接ＩＣカード１０へのアクセスを行わない場合は，ＩＣカード入出力装置２３は備えなくても良い。

【００３４】

図７はＩＣカード１０のハードウェア構成図である。ＩＣカード１０は，入出力部１１と，ＣＰＵ１２と，耐タンパー記憶装置１３と，耐タンパーメモリ１４と，がバスなどの内部通信線１５で連結されて構成されている。

【００３５】

本実施形態の証明書管理システムにおける処理フローについて説明する。以下に述べる処理フローは，各装置の記憶装置に格納されたプログラムがメモリにロードされ，ＣＰＵにより実行されることにより，証明書管理システムを構成する各装置，ＩＣカード上に具現化される各処理部により実行されるものである。また，各プログラムは予め記憶装置に格納されても良いし，他の記憶媒体または通信媒体（ネットワークまたはネットワークを伝搬する搬送波）を介して，必要なときに導入されても良い。

【００３６】

図８は，第１のサービス提供者装置40_1が信頼する認証局装置50_1がＩＣカード１

０に対して証明書を発行した後で，第２のサービス提供者装置４０$_2$が信頼する認証局装置５０$_2$がＩＣカード１０に対して証明書を発行するフロー図である。

【００３７】

なお，第１のサービス提供者装置４０$_1$が信頼する認証局装置５０$_1$がＩＣカード１０に対して証明書を発行した後では，ＩＣカード内で生成した秘密鍵Ａ１０１$_1$と公開鍵Ａ１０２$_1$のペア，および，該公開鍵Ａ１０２$_1$に対して，第１のサービス提供者装置４０$_1$が信頼する認証局装置５０$_1$が自身の秘密鍵Ａ５０１$_1$を用いて発行した証明書Ａ５０３$_1$，および，認証局装置５０$_1$自身の秘密鍵Ａ５０１$_1$に対応する自身の証明書Ａ５０２$_1$と，が，ＩＣカード内の第１のサービス提供者装置４０$_1$の領域に保存されている。

【００３８】

認証局装置５０$_2$において，上記鍵生成部５０５は，秘密鍵Ａ５０５$_2$と公開鍵Ａ５０６$_2$のペアを生成する（ステップＳ４０１）。

【００３９】

上記証明書発行申請生成部５０６は，ＩＣカード１０に対する証明書の発行申請を生成し，申請情報Ａ５０７$_2$と上記公開鍵Ａ５０６$_2$をＩＣカードに送信する（ステップＳ４０２）。

【００４０】

ＩＣカード１０において，証明書生成部１０２は，上記秘密鍵Ａ１０１$_1$を用いて認証局５０$_2$の証明書Ａ５０８$_2$を生成する（ステップＳ４０３）。

【００４１】

証明書生成部１０２は，上記証明書Ａ５０３$_1$と，上記証明書Ａ５０２$_1$と，上記ステップＳ４０３で生成した証明書Ａ５０８$_2$を，データ送受信部１０１を介して認証局装置５０$_2$に送信する。その後，端末２０は，ＩＣカード１０に対して，サービス提供者装置４０$_2$の領域を選択する（ステップＳ４０４）。

【００４２】

端末２０は，ＩＣカード１０に対して秘密鍵および公開鍵ペアの生成を依頼する（ステップＳ４０５）。

【００４３】

ＩＣカード１０において，上記鍵生成部１０４は，秘密鍵Ａ１０１$_2$および公開鍵Ａ１０２$_2$を生成し，上記ステップＳ４０４で選択された領域に保存する（ステップＳ４０６）。

【００４４】

ＩＣカード１０の鍵生成部１０４は，データ送受信部１０１を介して，端末２０に，上記生成した公開鍵Ａ１０２$_2$を送信する。端末２０は，上記公開鍵Ａ１０２$_2$と，証明書申請情報Ａ２０１$_2$と，を認証局装置５０$_2$に送信する（ステップＳ４０７）。

【００４５】

認証局装置５０$_2$において，上記証明書生成部５０２は，上記ステップＳ４０３で，ＩＣカードから発行された上記証明書Ａ５０８$_2$に対応した秘密鍵Ａ５０５$_2$を用いて証明書Ａ５０９$_2$を生成する（ステップＳ４０８）。

【００４６】

認証局装置５０$_2$において，通信部５０１は，該証明書Ａ５０９$_2$と，上記ステップＳ４０３で，ＩＣカードから受信した上記証明書Ａ５０８$_2$と，上記証明書Ａ５０３$_1$と，上記証明書Ａ５０２$_1$と，を端末２０に送信し，端末２０は，これらの証明書を受け取りＩＣカード１０に書き込む（ステップＳ４０９）。

【００４７】

ＩＣカード１０のデータ送受信部１０１は，受け取った，上記各証明書をステップＳ４０４で選択された領域に保存する（ステップＳ４１０）。

【００４８】

なお，ステップＳ４０３で発行する証明書には，公開鍵Ａ５０６$_2$以外にも，ＩＣカード情報や個人情報などの情報を含むようにしても良い。

【００４９】
また，ステップＳ４０６で秘密鍵Ａ１０１$_2$および公開鍵Ａ１０２$_2$を，ＩＣカード１０で生成するようにしているが，認証局装置５０$_2$で生成し，ＩＣカード１０内に保存するようにしても良い。
【００５０】
図９は，第２のサービス提供者装置４０$_2$が信頼する認証局装置５０$_2$が，ＩＣカード１０に対して発行した証明書Ａ５０９$_2$を検証するフロー図である。
【００５１】
端末２０からサービス提供要求を受けたサービス提供者装置４０$_2$において，上記証明書検証部４０２は，チャレンジ（たとえば乱数）Ａ４０１$_2$を生成し，端末２０に送信し，証明書要求を行う（ステップＳ５０１）。
【００５２】
端末２０は，ＩＣカード１０に対して，サービス提供者装置４０$_2$の領域を選択する（ステップＳ５０２）。
【００５３】
端末２０は，上記ステップＳ５０１でサービス提供者装置４０$_2$から送られたチャレンジＡ４０１$_2$を，ＩＣカード１０に送り暗号化を依頼する（ステップＳ５０３）。
【００５４】
ＩＣカード１０において，上記暗号化部１０５は，上記Ｓ５０２で選択された領域に保存されている秘密鍵Ａ１０１$_2$で，チャレンジＡ４０１$_2$を暗号化する（ステップＳ５０４）。
【００５５】
ＩＣカード１０のデータ送受信部１０１は，上記ステップＳ５０４で暗号化されたチャレンジＡ４０２$_2$と，上記ステップＳ５０４の暗号化で使用した秘密鍵Ａ１０１$_2$に対応した証明書Ａ５０９$_2$と，該証明書Ａ５０９$_2$の発行に使用した秘密鍵に対応した認証局装置５０$_2$の証明書Ａ５０８$_2$と，該証明書Ａ５０８$_2$の発行に使用したＩＣカード内の秘密鍵に対応した証明書Ａ５０３$_1$と，上記証明書Ａ５０２$_1$と，を端末２０に送信する。
【００５６】
端末２０は，ＩＣカード１０から受け取った，暗号化されたチャレンジＡ４０２$_2$と，上記各証明書と，をサービス提供者装置４０$_2$に転送する（ステップＳ５０５）。
【００５７】
サービス提供者装置４０$_2$において，上記証明書検証部４０２は，受け取った証明書Ａ５０９$_2$を使って，暗号化されたチャレンジＡ４０２$_2$を復号化し，上記ステップＳ５０１で送信したチャレンジＡ４０２$_2$と一致するかどうかを確認しチャレンジの検証を行う（ステップＳ５０６）。
【００５８】
サービス提供者装置４０$_2$において，上記証明書検証部４０２は，受け取った上記各証明書が失効されていないかどうかを確認するために，認証局装置５０$_1$および，認証局装置５０$_2$に対して証明書の失効情報の取得処理を行う（ステップＳ５０７）。
【００５９】
認証局装置５０$_1$および認証局装置５０$_2$は，ＩＣカード１０の利用者からの連絡に基づいて随時更新される上記失効情報ＤＢ５０４に基づいて，上記失効情報生成部５０３において失効情報を生成している。ステップ５０７における失効情報の要求に従い，証明書の失効情報を通知する（ステップＳ５０８）（ステップＳ５０９）。
【００６０】
サービス提供者装置４０$_2$において，上記証明書検証部４０２は，上記各証明書の検証処理を行う（ステップＳ５１０）。
【００６１】
検証に成功し，証明書は有効である，と判断した場合，上記サービス提供部４０３は，

サービスの提供を行う（ステップＳ５１１）。

【００６２】

なお，ステップＳ５１０において，証明書検証部４０２自らが証明書を検証しているが，外部の証明書検証機関に，検証を行いたい証明書を送信し，証明書の有効性の問い合わせをするようにしても良い。

【００６３】

図１０は，上記証明書検証ステップ（Ｓ５１０）を詳細に説明するためのフロー図である。

【００６４】

上記認証局装置５０$_2$が発行した証明書Ａ５０９$_2$の有効性の検証を行う（ステップＳ６０１）。具体的には上記ステップＳ５０８で通知された失効情報Ａ５０４$_2$に失効された記載が無いか確認するとともに，上記証明書Ａ５０９$_2$を発行するときに使用した秘密鍵に対応した認証局装置５０$_2$の証明書Ａ５０８$_2$に含まれる公開鍵を使用し，上記証明書Ａ５０９$_2$に記述されているディジタル署名を検証する。失効されていない，かつ，ディジタル署名が有効である，ならば次のステップを実行する。そうでなければ，証明書Ａ５０９$_2$は無効であると判断する。

【００６５】

上記ＩＣカード１０が発行した証明書Ａ５０８$_2$の有効性の検証を行う（ステップＳ６０３）。具体的には上記ステップＳ５０８で通知された失効情報Ａ５０４$_2$に失効された記載が無いか確認するとともに，上記証明書Ａ５０８$_2$を発行するときに使用した秘密鍵に対応した認証局装置５０$_1$が，ＩＣカードに対して発行した証明書Ａ５０３$_1$に含まれる公開鍵を使用し，上記証明書Ａ５０８$_2$に記述されているディジタル署名を検証する。失効されていない，かつ，ディジタル署名が有効である，ならば次のステップを実行する。そうでなければ，上記証明書Ａ５０８$_2$は無効であり，同時に証明書Ａ５０９$_2$は無効であると判断する。

【００６６】

上記認証局装置５０$_1$が発行した証明書Ａ５０３$_1$の有効性の検証を行う（ステップＳ６０５）。具体的には上記ステップＳ５０９で通知された失効情報Ａ５０４$_1$に失効された記載が無いか確認するとともに，上記証明書Ａ５０３$_1$を発行するときに使用した秘密鍵に対応した認証局装置５０$_1$の証明書Ａ５０２$_1$に含まれる公開鍵を使用し，上記証明書Ａ５０３$_1$に記述されているディジタル署名を検証する。失効されていない，かつ，ディジタル署名が有効である，ならば次のステップを実行する。そうでなければ，上記証明書Ａ５０３$_1$は無効であり，同時に上記証明書Ａ５０８$_2$は無効であり，同時に証明書Ａ５０９$_2$は無効であると判断する。

【００６７】

上記認証局装置５０$_1$が発行した証明書Ａ５０２$_1$の有効性の検証を行う（ステップＳ６０７）。上記ステップＳ５０９で通知された失効情報Ａ５０４$_1$に失効された記載が無いか確認する。証明書Ａ５０２$_1$は，サービス提供者装置４０$_2$が信頼する認証局装置の証明書なので，証明書Ａ５０２$_1$が失効されていなければ，証明書Ａ５０２$_1$は有効であると判断し，同時に

上記証明書Ａ５０３$_1$は有効であり，上記証明書Ａ５０８$_2$は有効であり，同時に証明書Ａ５０９$_2$は有効であると判断する（ステップＳ６０９）。

【００６８】

そうでなければ，証明書Ａ５０２$_1$は無効であると判断し，同時に上記証明書Ａ５０３$_1$は無効であり，上記証明書Ａ５０８$_2$は無効であり，同時に証明書Ａ５０９$_2$は無効であると判断する（ステップＳ６１０）。

【００６９】

なお，上述の各有効性確認ステップ（Ｓ６０１，Ｓ６０３，Ｓ６０５，Ｓ６０７）の順序は入れ替えても良い。

【００７０】

上述のように，本実施例では，証明書Ａ５０９$_2$の有効性を検証するためには，証明書Ａ５０８$_2$および証明書Ａ５０２$_1$の有効性の検証が必要となるように，証明書の連鎖を構成している。この連鎖構造により，ＩＣカードを無くした等，何らかの理由により，証明書Ａ５０９$_2$および証明書Ａ５０２$_1$を失効させたい場合，上位の証明書Ａ５０２$_1$を失効させる処理を行えば，証明書Ａ５０９$_2$を失効させる処理を行わなくても，証明書Ａ５０９$_2$も失効させることができる。

【００７１】

一方，各証明書の検証時には，その発行元認証局が発行した失効情報Ａ５０４$_1$とＡ５０４$_2$を参照するように構成している。この構成により，証明書Ａ５０９$_2$および／または証明書Ａ５０２$_1$を個々に失効させることも可能である。例えば，サービス提供者装置４０$_2$が提供するサービスを停止する場合などには，サービス提供者装置４０$_2$が信頼する認証局装置による失効情報を発行させればよい。これにより，サービス提供者装置４０$_1$が信頼する認証局装置５０$_1$が発行した証明書は有効のまま，サービス提供者装置４０$_2$が信頼する認証局装置５０$_2$から発行された証明書Ａ５０９$_2$を失効させることが可能となる。

【００７２】

なお，本発明は，上記の本実施形態に限定されるものではなく，その要旨の範囲内で様々な変形が可能である。

【００７３】

たとえば，認証局装置から発行された証明書，および，認証局装置の証明書を，ＩＣカード内に保存するようにしているが，たとえばディレクトリサーバのようなＩＣカード外のサーバ装置を証明書保管機関装置として設けて，証明書を保管するようにしてもよい。その場合には，図８および図９で示したフローで証明書を送りあう代わりに，証明書保管機関装置の保管場所の情報を送りあうようにすれば良い。また，送りあう情報を暗号化するようにしても良い。

【００７４】

また，ＩＣカード１０の内部データは，暗号化されて保存するようにしても良い。

【００７５】

また，本実施例では，第２の証明書（Ａ５０９$_2$）を発行するのは，第２のサービス提供者装置４０$_2$が信頼する認証局装置５０$_2$としているが，第１のサービス提供者装置４０$_1$が信頼する認証局装置５０$_1$が，第２の証明書（Ａ５０９$_2$）を発行しても良い。

【００７６】

また，本実施例の応用例として，
複数のサービス提供者装置４０$_n$（ｎ≧２）がサービスを提供するために，ＩＣカード１０が，上位の認証局装置である第１の認証局装置５０$_1$が発行した証明書Ａ５０３$_1$と対応する秘密鍵Ａ１０１$_1$とを用いて，複数の下位の認証局である第ｎ（ｎ≧２）の認証局装置５０$_n$の証明書Ａ５０８$_n$を生成し，さらに，該証明書Ａ５０８$_n$と対応する秘密鍵Ａ５０５$_n$とを用いて，第ｎの認証局装置５０$_n$が証明書Ａ５０９$_n$を発行するように構成しても良い。

【００７７】

また，第ｍ（ｍ≧２）の認証局装置５０$_m$が発行した証明書Ａ５０３$_m$と対応する秘密鍵Ａ１０１$_m$とを用いて第ｎ（ｎ＞ｍ）の認証局装置５０$_n$の証明書Ａ５０８$_n$を生成し，さらに，該証明書Ａ５０８$_n$と対応する秘密鍵Ａ５０５$_n$とを用いて，第ｎの認証局装置５０$_n$が証明書Ａ５０９$_n$を発行するようにしても良い。

【図面の簡単な説明】

【００７８】

【図１】本発明の一実施形態が適用された証明書管理システムのネットワーク構成を説明するための図である。

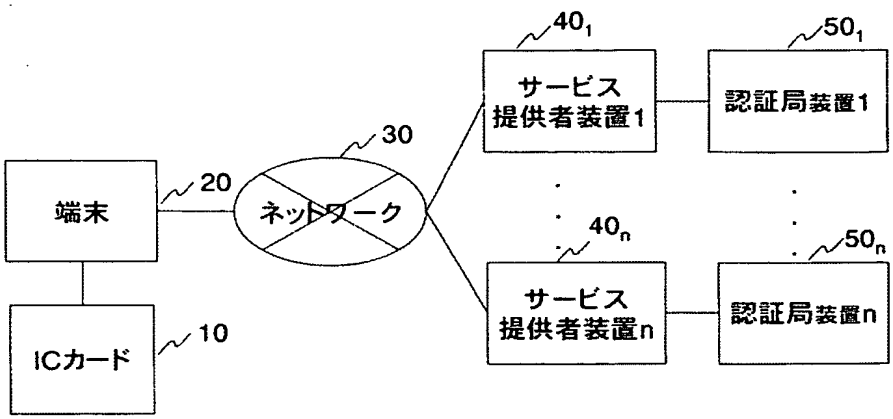
【図２】認証局装置の構成例を示すための図である。

【図３】図１に示すサービス提供者装置の構成例を示すための図である。

【図４】図１に示すＩＣカードの構成例を示すための図である。
【図５】図１に示す端末の構成例を示すための図である。
【図６】図１に示す端末のハードウェア構成を示す図である。
【図７】図１に示すＩＣカードのハードウェア構成を示す図である。
【図８】本発明の一実施形態が適用された証明書管理システムの証明書発行を説明するフロー図である。
【図９】本発明の一実施形態が適用された証明書管理システムの証明書検証を説明するフロー図である。
【図１０】図９の証明書検証ステップを詳しく説明するフロー図である。
【符号の説明】
【００７９】
１０・・・ＩＣカード，１１・・・入出力装置，１２・・・ＣＰＵ，１３・・・記憶装置，１４・・・メモリ，１５・・・内部通信線，２０・・・端末，２１・・・通信装置，２２・・・入出力装置，２３・・・ＩＣカード入出力装置，２４・・・記憶装置，２５・・・ＣＰＵ，２６・・・メモリ，２７・・・読取装置，２８・・・記憶媒体，２９・・・内部通信線，３０・・・ネットワーク，40_1～40_n・・・サービス提供者装置，50_1～50_n・・・認証局装置，１０１・・・データ送受信部，１０２・・・証明書生成部，103_1～103_nサービス提供者固有領域，１０４・・・鍵生成部，１０５・・・暗号化部，１０６・・・サービス提供者認証部，２０１・・・ＩＣカードアクセス部，２０２・・・データ送受信部，４０１・・・通信部，４０２・・・証明書検証部，４０３・・・サービス提供部，５０１・・・通信部，５０２・・・証明書生成部，５０３・・・失効情報生成部，５０４・・・失効情報データベース，５０５・・・鍵生成部，５０６・・・証明書発行申請生成部，$A101_1$・・・秘密鍵，$A101_2$・・・秘密鍵，$A102_1$・・・公開鍵，$A102_2$・・・公開鍵，$A201_1$・・・申請情報，$A201_2$・・・申請情報，$A502_1$・・・認証局装置50_1の証明書，$A503_1$・・・認証局装置50_1発行の証明書，$A401_1$・・・チャレンジ，$A401_2$・・・チャレンジ，$A402_1$・・・暗号化されたチャレンジ，$A402_2$・・・暗号化されたチャレンジ，$A504_1$・・・失効情報，$A504_2$・・・失効情報，$A505_2$・・・秘密鍵，$A506_2$・・・公開鍵，$A507_2$・・・申請情報，$A508_2$・・・$A503_1$に対応した秘密鍵で生成した証明書，$A509_2$・・・認証局装置50_2発行の証明書。

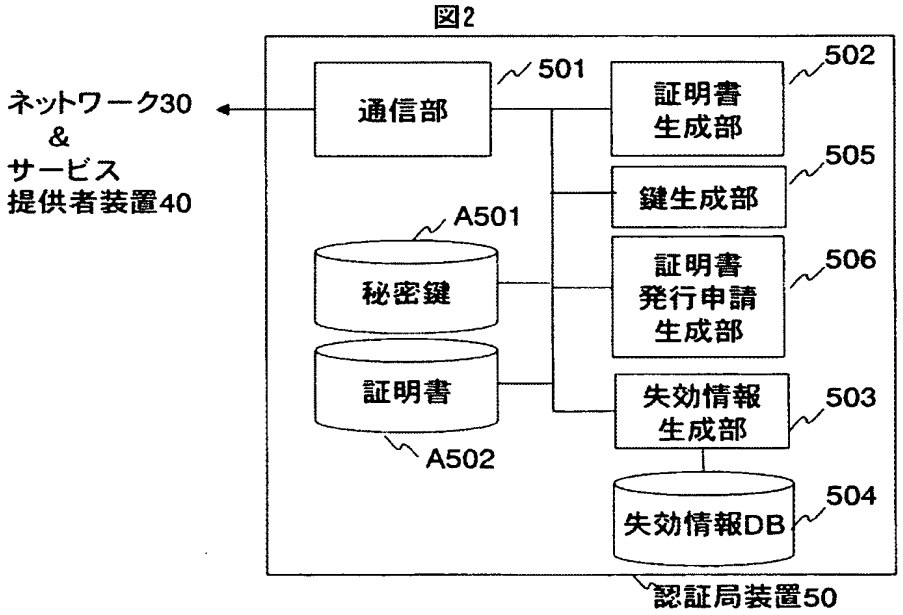
【書類名】図面
【図１】

図1



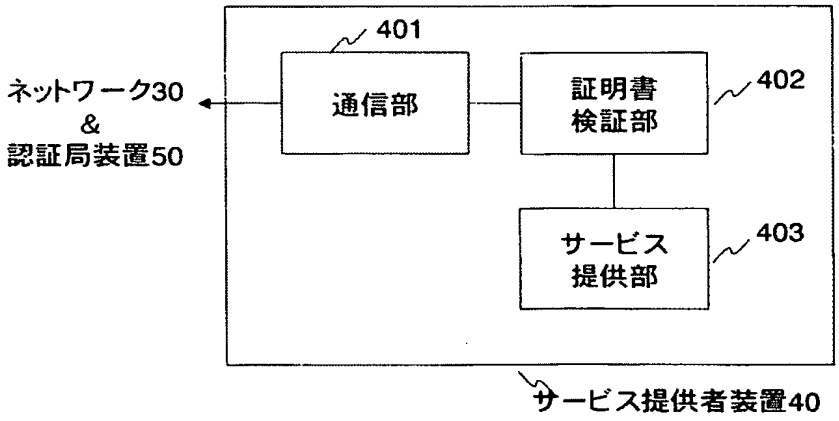
【図２】

図2



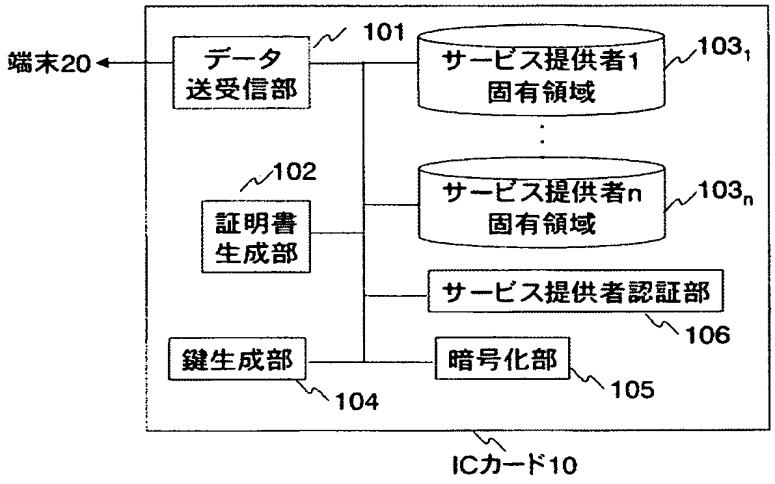
【図３】

図3



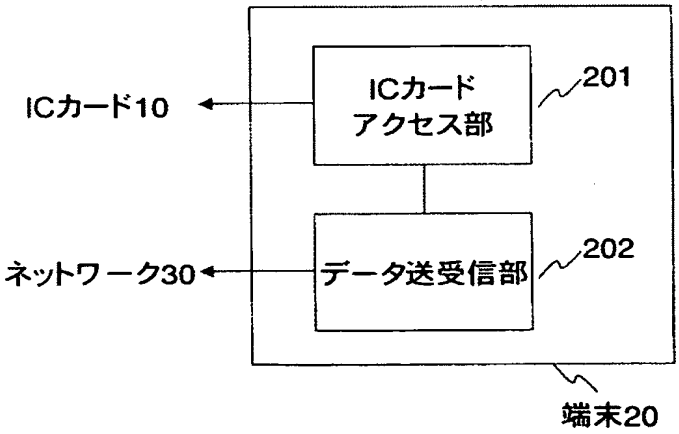
【図４】

図4



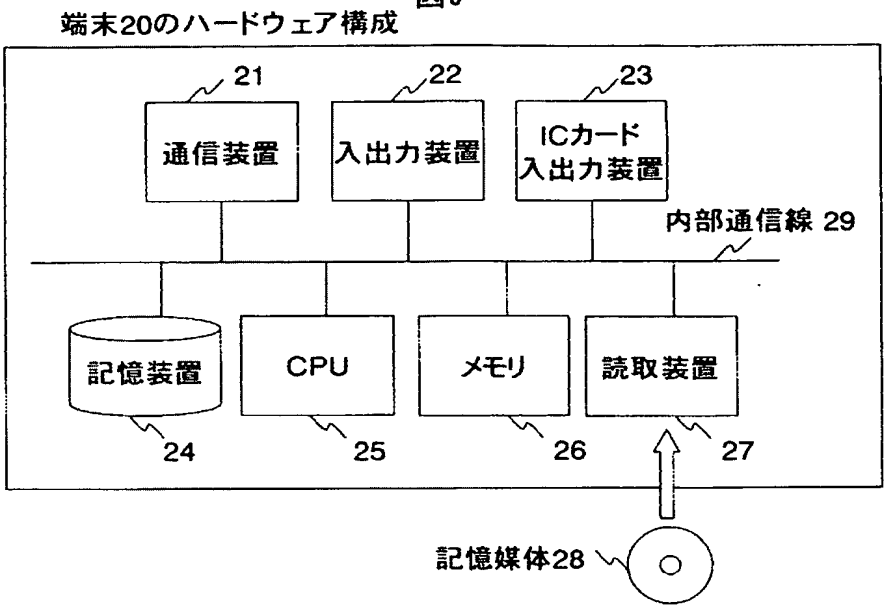
【図５】

図5



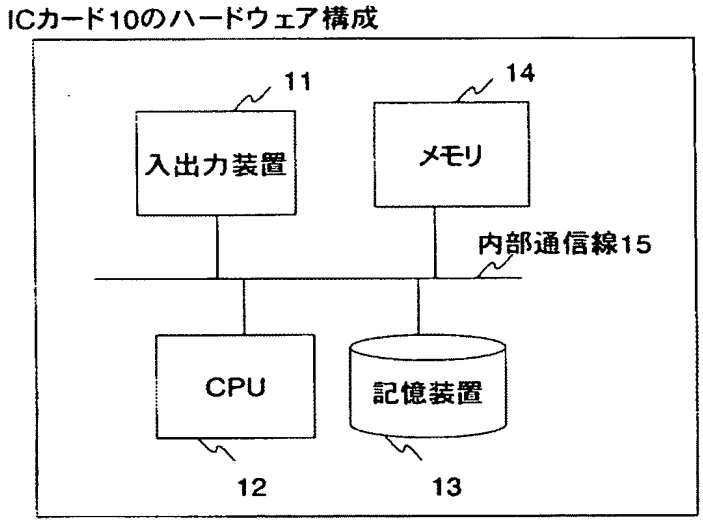
【図６】

図6


端末20のハードウェア構成
21
22
23
通信装置
入出力装置
ICカード
入出力装置
内部通信線 29
記憶装置
CPU
メモリ
読取装置
24
25
26
27
記憶媒体28

【図７】

図7


ICカード10のハードウェア構成
11
14
入出力装置
メモリ
内部通信線15
CPU
記憶装置
12
13

【図８】

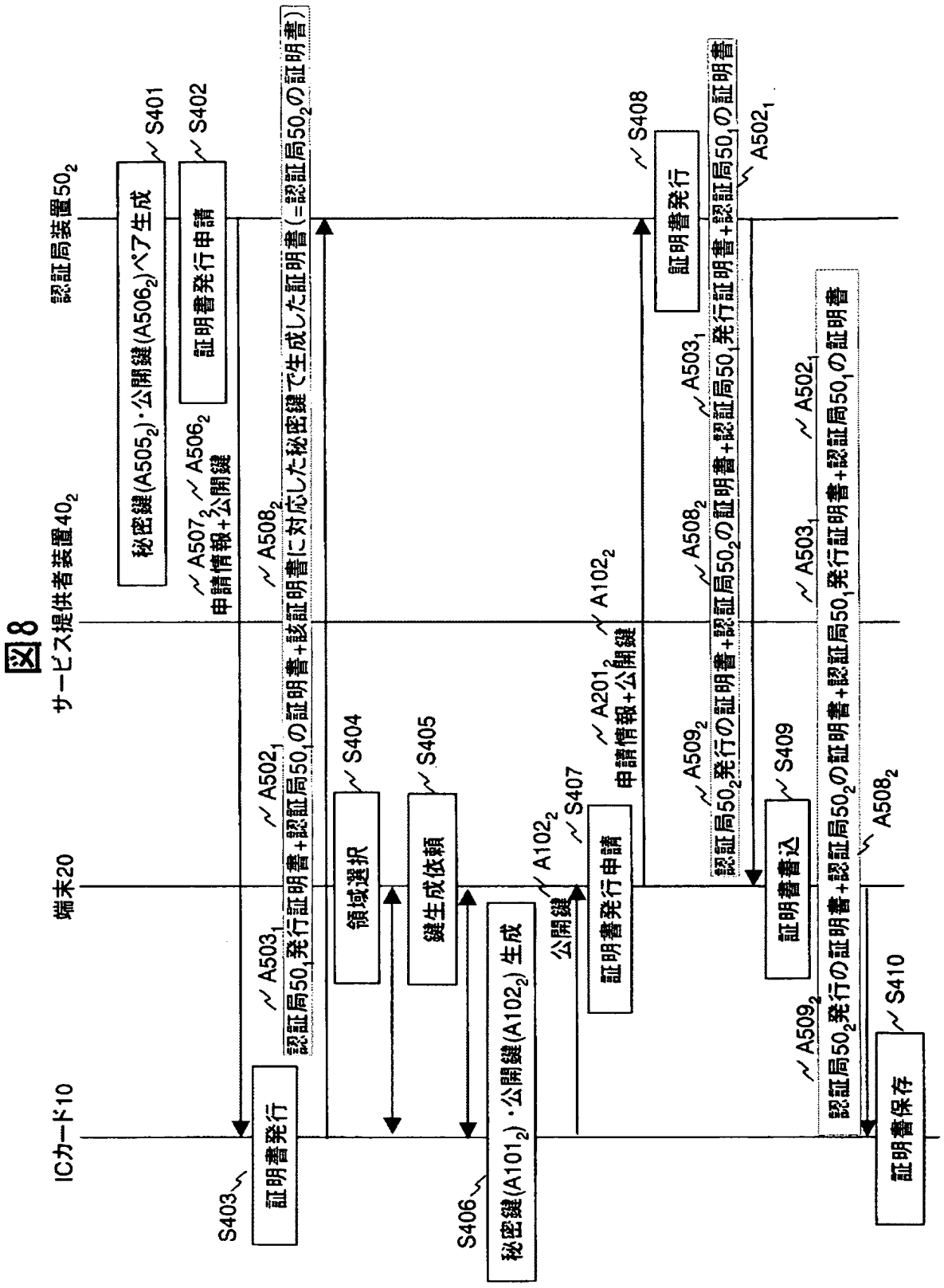


図8
ICカード10
端末20
サービス提供者装置40$_2$
認証局装置50$_2$
秘密鍵(A505$_2$)・公開鍵(A506$_2$)ペア生成
S401
証明書発行申請
S402
A507$_2$ 申請情報+A506$_2$公開鍵
A508$_2$
認証局50$_1$発行証明書+認証局50$_2$の証明書+該証明書に対応した秘密鍵で生成した証明書(=認証局50$_2$の証明書)
A502$_1$
A503$_1$
証明書発行
S403
領域選択
S404
鍵生成依頼
S405
秘密鍵(A101$_2$)・公開鍵(A102$_2$)生成
S406
A102$_2$ 公開鍵
S407
A201$_2$ 申請情報+公開鍵
証明書発行申請
A102$_2$
S408
証明書発行
A503$_1$
A508$_2$
認証局50$_2$発行の証明書+認証局50$_2$の証明書+認証局50$_1$発行証明書+認証局50$_1$の証明書
A502$_1$
A509$_2$
証明書書込
S409
A503$_1$
A508$_2$
認証局50$_2$発行の証明書+認証局50$_2$の証明書+認証局50$_1$発行証明書+認証局50$_1$の証明書
A502$_1$
A509$_2$
証明書保存
S410

【図９】

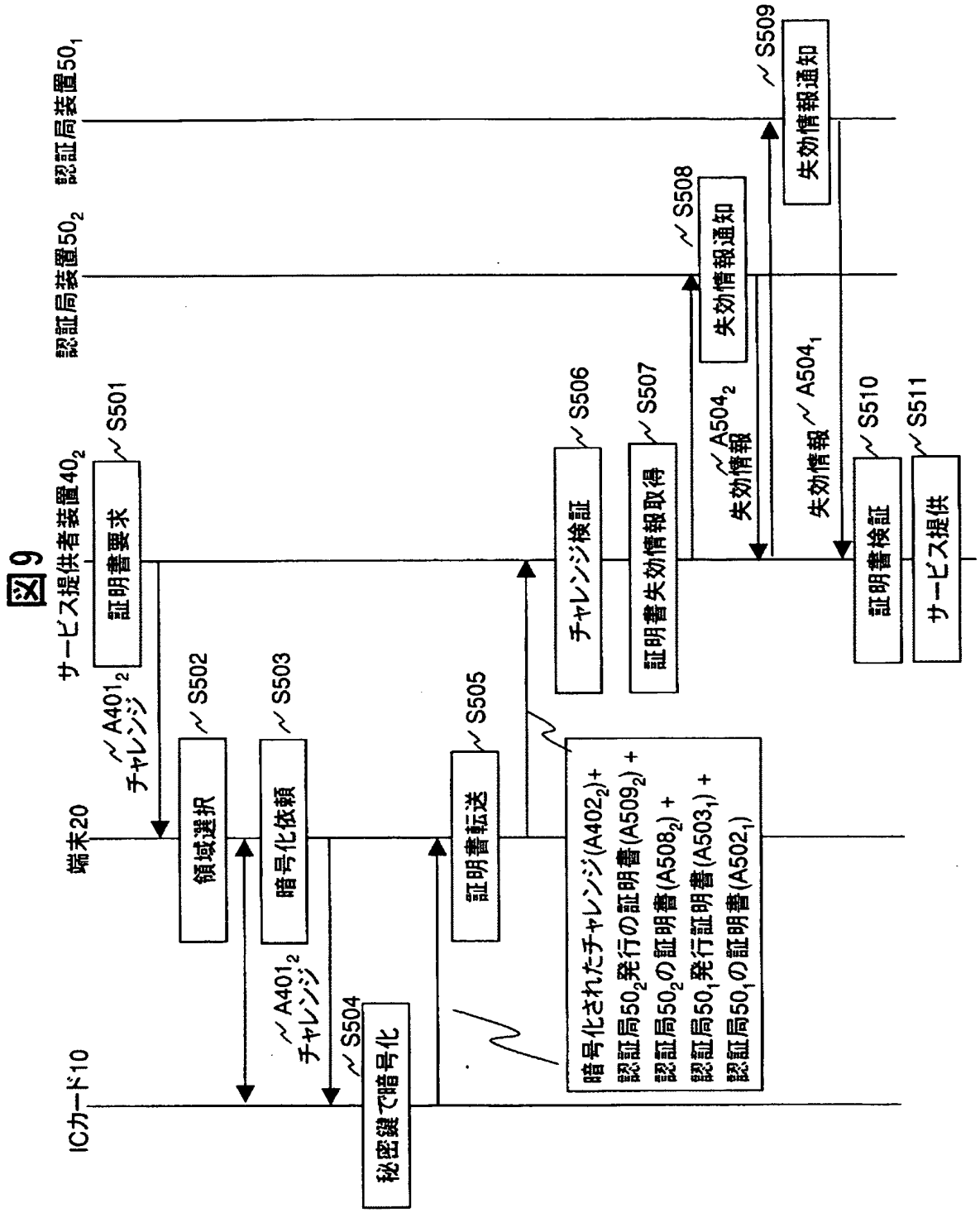
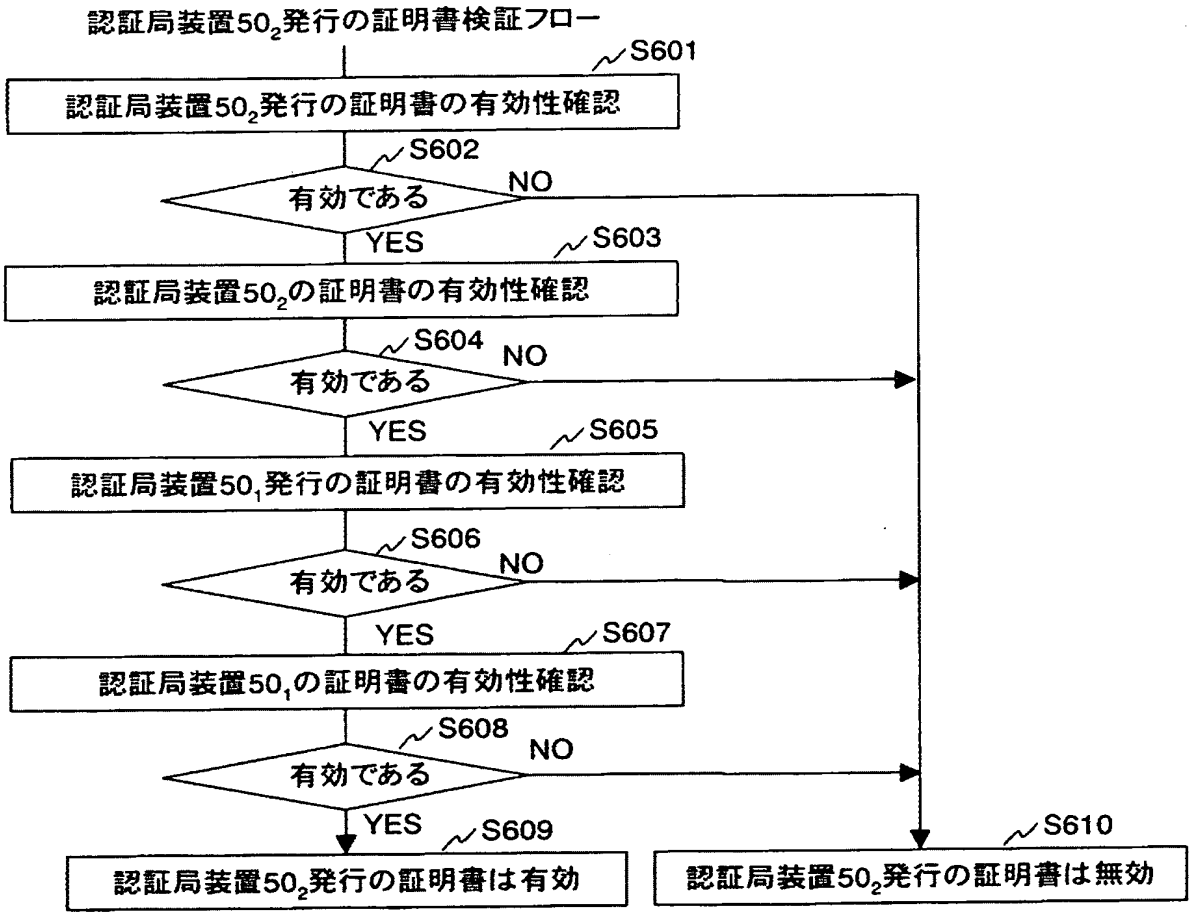


図9
サービス提供者装置40₂
認証局装置50₂
認証局装置50₁
端末20
ICカード10
証明書要求
S501
A401₂ チャレンジ
領域選択
S502
暗号化依頼
S503
A401₂ チャレンジ
S504
秘密鍵で暗号化
証明書転送
S505
暗号化されたチャレンジ(A402₂)+認証局50₂発行の証明書(A509₂)+認証局50₂の証明書(A508₂)+認証局50₁発行証明書(A503₁)+認証局50₁の証明書(A502₁)
チャレンジ検証
S506
証明書失効情報取得
S507
失効情報通知
S508
A504₂ 失効情報
失効情報通知
S509
A504₁ 失効情報
証明書検証
S510
サービス提供
S511

【図１０】

図10


認証局装置50$_2$発行の証明書検証フロー
S601
認証局装置50$_2$発行の証明書の有効性確認
S602
有効である
NO
YES
S603
認証局装置50$_2$の証明書の有効性確認
S604
有効である
NO
YES
S605
認証局装置50$_1$発行の証明書の有効性確認
S606
有効である
NO
YES
S607
認証局装置50$_1$の証明書の有効性確認
S608
有効である
NO
YES
S609
認証局装置50$_2$発行の証明書は有効
S610
認証局装置50$_2$発行の証明書は無効

【書類名】要約書
【要約】
【課題】
複数のサービス提供者装置が，それぞれ異なる信頼する認証局装置から発行される証明書を，ＩＣカードに搭載される場合に，第一のサービス提供者装置が信頼する認証局装置が発行した証明書を失効させるだけで，すべての証明書を失効させることができ，また，個々の証明書を個別に失効させることができる，証明書管理方法およびその方法が適用されるシステムを提供する。
【解決手段】
認証局ｎ（ｎ≧２）は，ＩＣカードに事前に搭載済みの認証局１から発行された証明書１と対応する秘密鍵１を用いて生成された証明書ｎ’と対応する秘密鍵ｎ’を用いて，証明書ｎを発行する。すべての証明書を失効させたい場合は，認証局１から発行された証明書１を失効させる。
【選択図】　図４

認定・付加情報

特許出願の番号	特願２００３－４０２４０１
受付番号	５０３０１９８２４４１
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年１２月　３日

＜認定情報・付加情報＞

【提出日】　平成15年12月 2日

特願２００３－４０２４０１

出　願　人　履　歴　情　報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所